certain way. Note that the token offers only limited security, since network addresses can of course be duplicated, or the Bluetooth device of a secure KD can be removed and planted in an unsecure device. However, the token scheme significantly raises the effort needed to commit fraudulent acts, since a KD cannot then be compromised using software alone. The system then compares favorably to traditional paper tickets which are easy to forge. Note also that copied tickets are a problem only if the ticket has a limited number of uses, there are several lock devices where they can be used, the lock devices cannot constantly communicate with each other to share information about ticket use, and fraud detection after the fact is not sufficient.

The advantage of placing user authenticating information on the KD is that the information can be used by different, independent LDs to authenticate the user. The disadvantage is that if a KD is stolen, the information could conceivably be read from it. Also, owners of other LDs would know the information since the user has to enter it when opening an LD. Thus, only information like fingerprints and retinal scans, which are known by other LDs that use similar security features in any case, should be stored unencrypted on the KD. The information should still be digitally signed, together with the KID, by some well-known trusted authority to guard against stolen KDs whose authentication information has been overwritten with counterfeited information.

Authentication information like access codes, that depend on the information being secret, should be encrypted by the LD that stores it on the KD. The information cannot then be generally used, but it is still useful, since it can be used by different LDs which are owned by the same authority but do not have contact with each other (other than sharing the same encryption key).

It should be noted that even storing unencrypted and unsigned authentication information on the KD is still a valuable security feature, since even if the KD is stolen, reading or counterfeiting the information requires technical knowledge and equipment unavailable to most criminals. For example, a fingerprint stored on the KD in unencrypted form significantly enhances security for LDs that have fingerprint scanning capability.

An LD consists of a power source, a processing unit, storage (volatile and non-volatile memory), a communication device (preferably a Bluetooth wireless communication device), and (assuming the LD is installed as a door lock) a device that mechanically locks and unlocks the door. An LD may also have an emergency power socket for KDs that have run out of power. An LD may further have input devices for reading user authentication information, such as keypads, fingerprint or retinal scanning devices, etc. An LD stores the following information:

- A unique lock device identifier, hereafter LID. A LID must be changeable to support the copying of locks.
- A human-readable name for the lock.
- A Confirm flag that specifies whether users should confirm unlocking the door by operating the confirmation input device on the KD.
- A code used for controlling the LD, hereafter LD PIN code.
- For each KD that can open the LD:
    - KID.
    - User name.
    - Bluetooth Link key.
    - KD public key.

- Access rights (e.g. time period when the KD has access, whether the KD is authorized to create new keys or tickets, what kind (e.g. almost one-day) of tickets the KD can create if any, whether they KD is authorized to perform key management operations on the lock device).

Optionally, an LD may also store the following information:

- User authenticating information, such as access codes, fingerprints, retinal scans, etc., to guard against stolen KDs. Note that this information could also be stored on the KD.
- A key for encrypting and decrypting the above information when they are stored on a KD.
- A list of untrusted public keys and ticket identifiers (hereafter blacklist, see below). Any ticket that contains one of these public keys or ticket identifiers is invalid. Also, any KD whose public key is in this list cannot store its public key on the LD.

When adding a key to this list, any KD with that public key must also be removed from the LD's KD database. Additionally, each ticket identifier on the blacklist may have a validity date, after which the ticket is invalid in any case. This allows obsolete information to be purged from the blacklist. Furthermore, a ticket identifier on the blacklist may have a counter that gives the number of times the ticket has been used. This allows tickets that can be used *n* times. These tickets are still valid, until the use counter reaches the maximum number of allowed uses.

Link keys are used by Bluetooth for authentication. Normally, Unit keys of KDs are used. This allows the KD to authenticate an LD as one of the LDs it has stored its Unit